Security of Personal Data Processing Event

Data Protection by design for SMEs

Notifying personal data breaches

Dr. Konstantinos Limniotis

Hellenic Data Protection Authority

klimniotis at dpa.gr

Athens, October 8th , 2018

Overview

- A new obligation for the data controllers
  - Data processors should be also aware of this obligation

- What is a personal data breach?

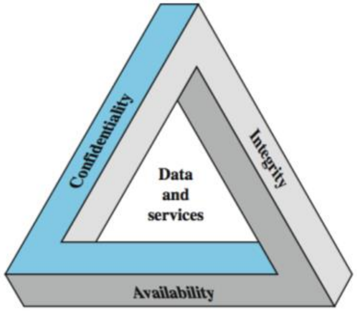
- When and how is being notified to the Data Protection Authority?

- When is being communicated to the affected individuals?

- What a DPA is "expecting to see"?

Introduction - Definitions

- (Personal) data security goals
  - Confidentiality
  - Integrity
  - Availability

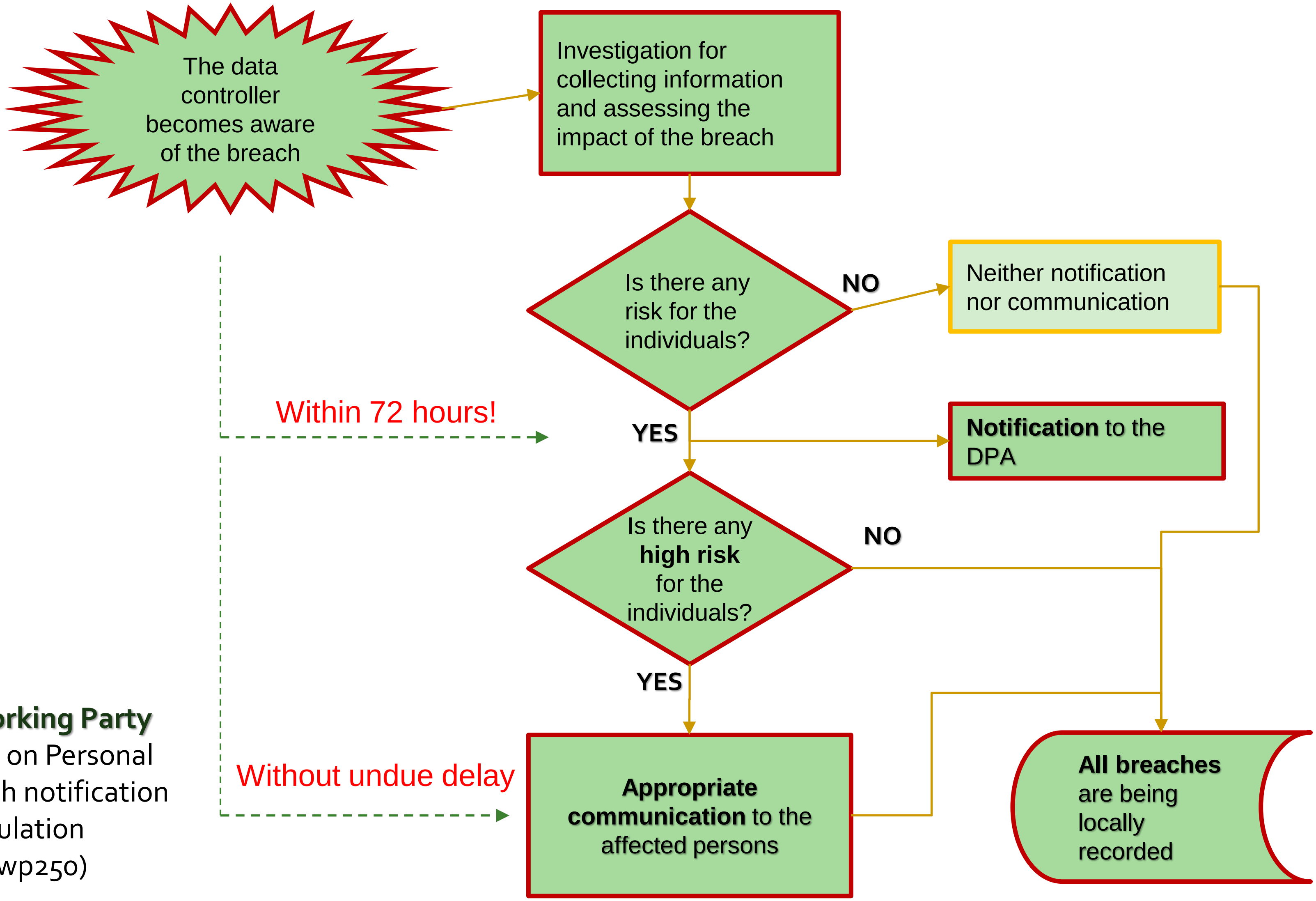


- **Personal data breach**: breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
  - Confidentiality breach
  - Integrity breach
  - Availability breach

  or a combination…

- What the GDPR brings (art. 33 & 34)
  - The data controller should document all personal data breaches
  - The data controller should notify the breach to the competent Data Protection Authority (unless it is unlikely to result in a risk to the rights and freedoms of natural persons)
  - The data controller should communicate the breach to the affected individuals in case that it is likely to result in a **high risk** to the rights and freedoms of them

The overall process


The data controller becomes aware of the breach

Investigation for collecting information and assessing the impact of the breach

Is there any risk for the individuals?

NO

Neither notification nor communication

Within 72 hours!

YES

Notification to the DPA

Is there any **high risk** for the individuals?

NO

YES

Without undue delay

Appropriate communication to the affected persons

All breaches are being locally recorded

Art. 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679 (wp250)

Examples (WP29 guidelines)

INCIDENT			
A controller stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in. The decryption key has not been compromised	NO	NO	Things would be different if the decryption key was also stolen
Personal data of individuals are exfiltrated from a secure (https) website managed by the controller during a cyber-attack.	YES	HIGHLY PROBABLE	
A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	NO	NO	
A controller suffers a ransomware attack (data were encrypted). No back-ups are available and the data cannot be restored. On investigation, it becomes clear that there was no other malware present in the system.	YES	YES	Things would be different if backup was present
An individual phones the controller's call centre to report a data breach. The individual has received a monthly statement (financial data) for someone else.	YES	YES	Only the single individual affected
An online marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	YES	YES	
Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	YES	YES	

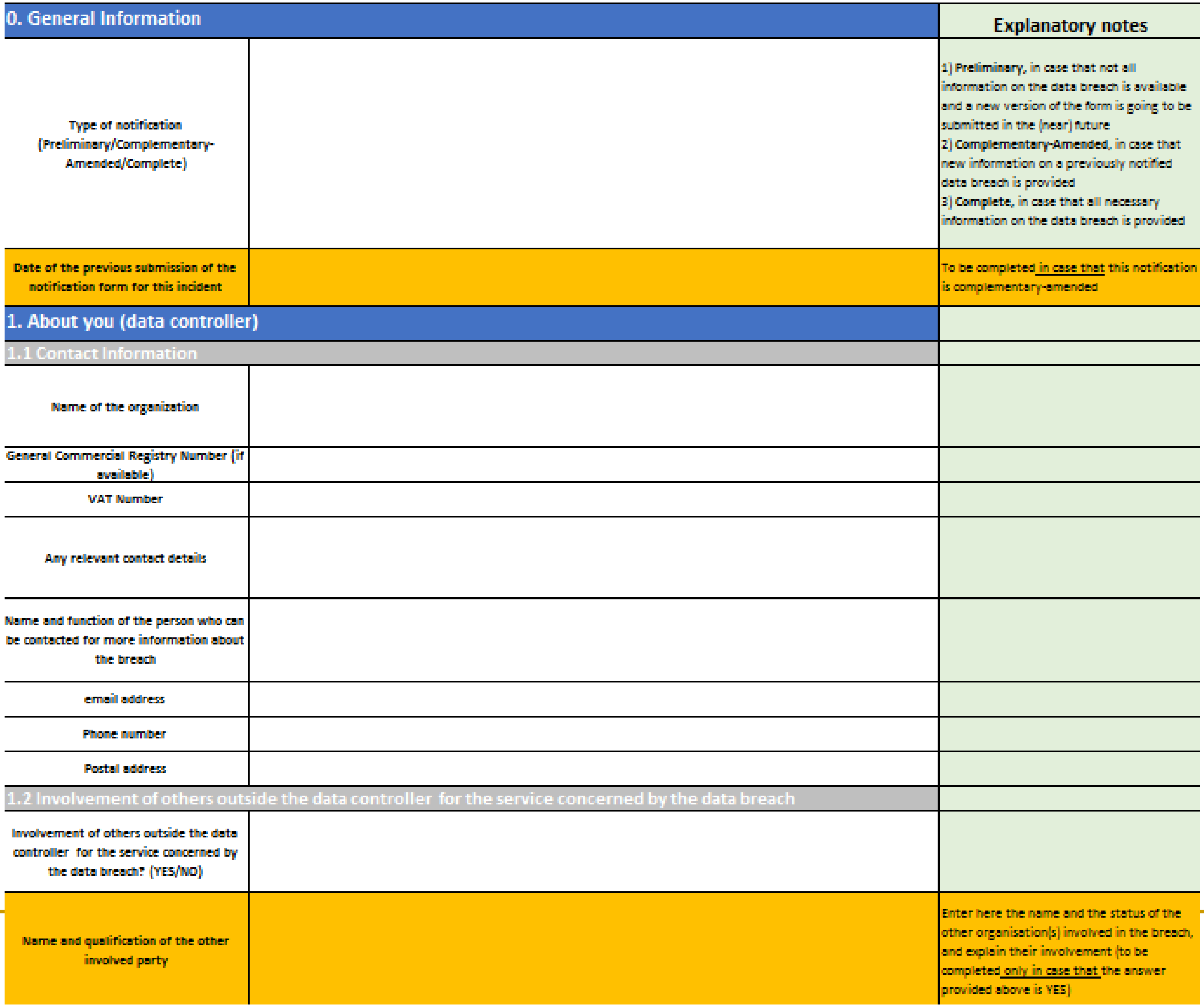
What is to be notified to the DPA

- The nature of the breach
  - Categories and approximate number of data subjects concerned,….
- The possible consequences
- The measures taken or proposed to be taken to address the breach
- Whether the data subjects have been informed or not
  - Important to assess in time whether high risks are present
  - The DPA may require such a communication to the affected individuals in any case

- If no all required information is available, the notification may be in phases
  - So as to ensure that the notification is being submitted within 72 hours

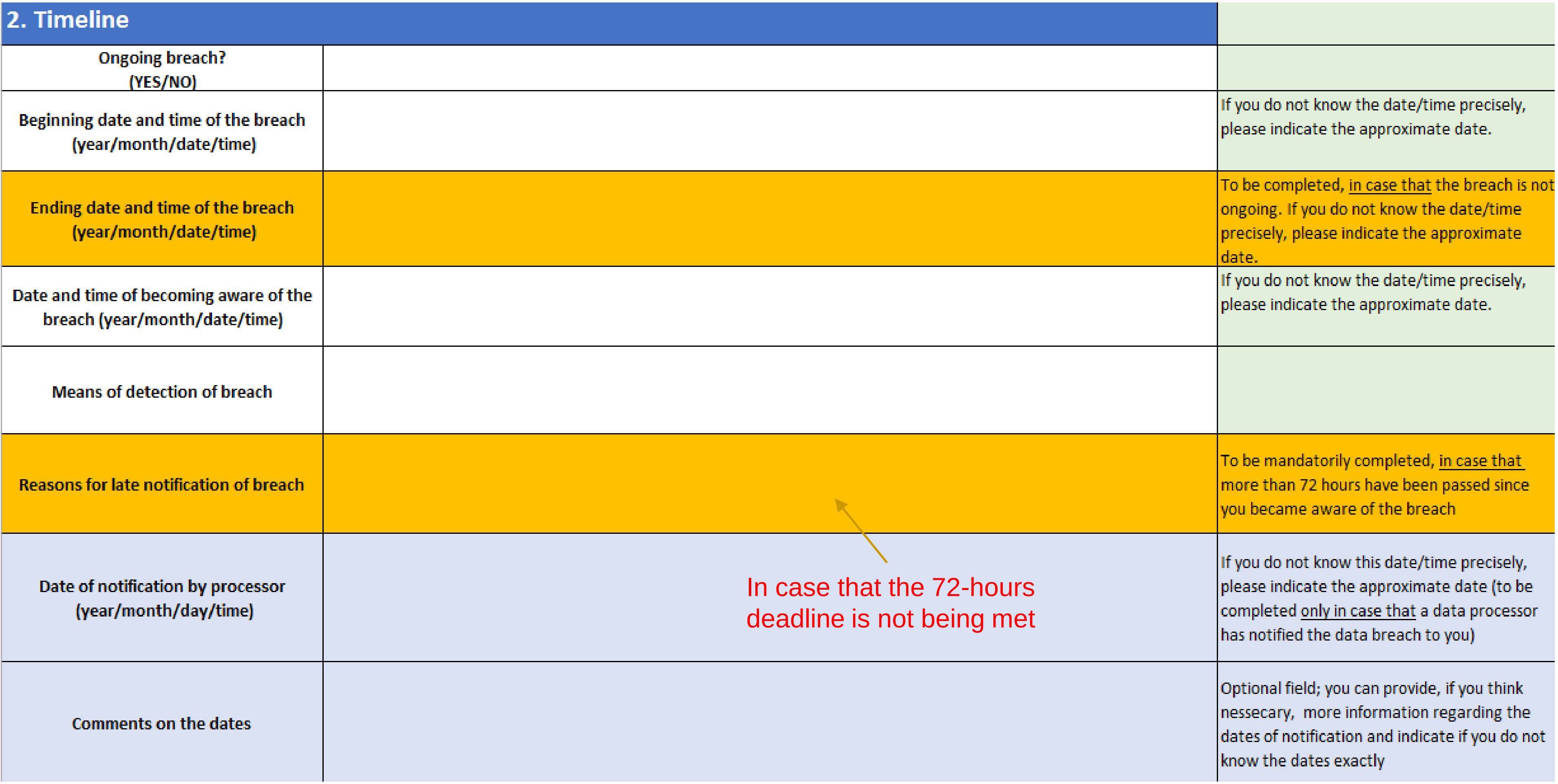
- => Necessary for any data controller to determine procedures for detecting and handling personal data breaches
  - The role of the data processor is also important

The data breach notification form



0. General Information		**Explanatory notes**
Type of notification (Preliminary/Complementary-Amended/Complete)		1) **Preliminary**, in case that not all information on the data breach is available and a new version of the form is going to be submitted in the (near) future 2) **Complementary-Amended**, in case that new information on a previously notified data breach is provided 3) **Complete**, in case that all necessary information on the data breach is provided
Date of the previous submission of the notification form for this incident		To be completed in case that this notification is complementary-amended
1. About you (data controller)		
1.1 Contact Information		
Name of the organization		
General Commercial Registry Number (if available)		
VAT Number		
Any relevant contact details		
Name and function of the person who can be contacted for more information about the breach		
email address		
Phone number		
Postal address		
1.2 Involvement of others outside the data controller for the service concerned by the data breach		
Involvement of others outside the data controller for the service concerned by the data breach? (YES/NO)		
Name and qualification of the other involved party		Enter here the name and the status of the other organisation(s) involved in the breach, and explain their involvement (to be completed only in case that the answer provided above is YES)

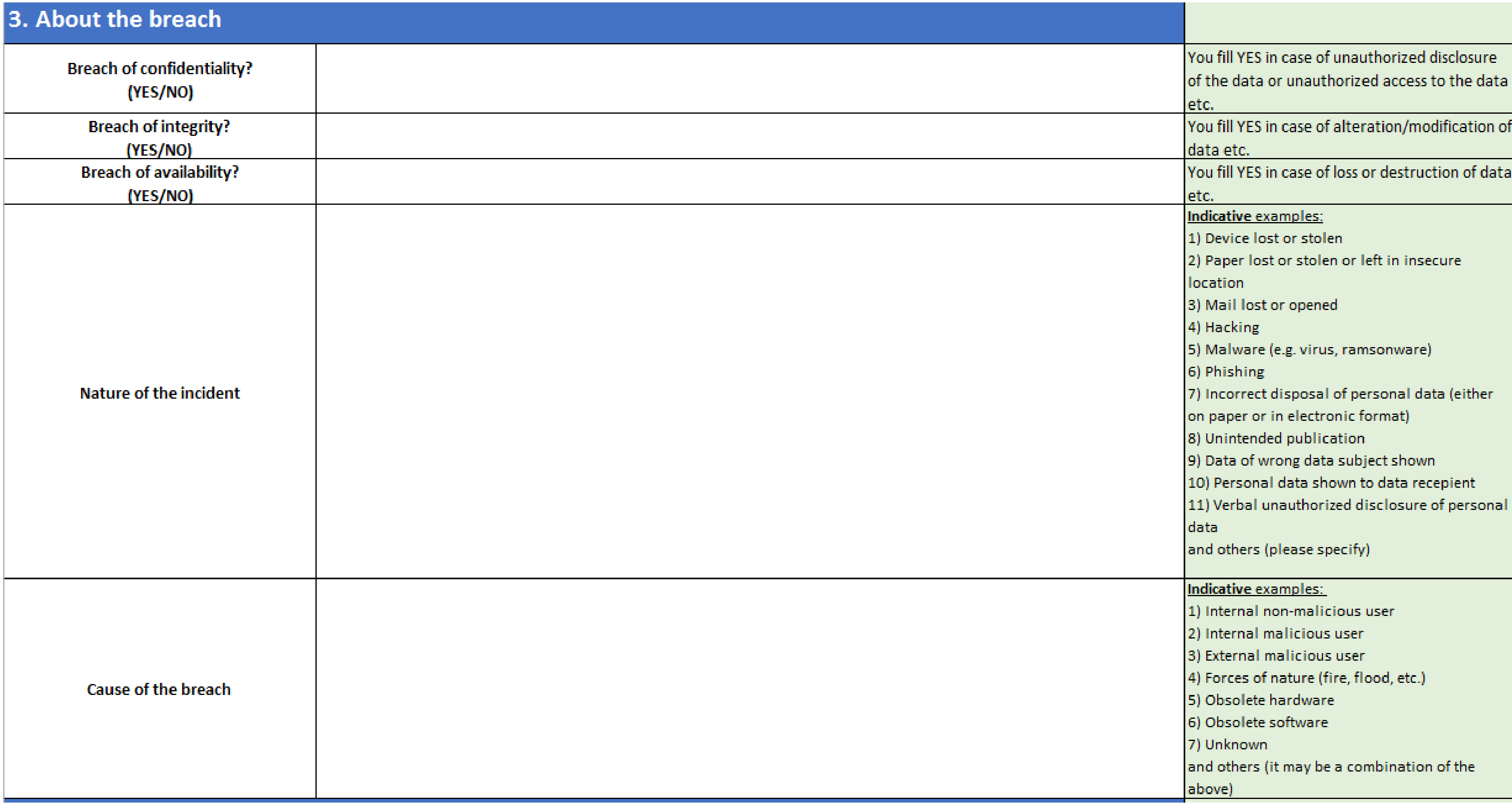
The data breach notification form (cont.)



2. Timeline		
Ongoing breach? (YES/NO)		
Beginning date and time of the breach (year/month/date/time)		If you do not know the date/time precisely, please indicate the approximate date.
Ending date and time of the breach (year/month/date/time)		To be completed, in case that the breach is not ongoing. If you do not know the date/time precisely, please indicate the approximate date.
Date and time of becoming aware of the breach (year/month/date/time)		If you do not know the date/time precisely, please indicate the approximate date.
Means of detection of breach		
Reasons for late notification of breach		To be mandatorily completed, in case that more than 72 hours have been passed since you became aware of the breach
Date of notification by processor (year/month/day/time)		If you do not know this date/time precisely, please indicate the approximate date (to be completed only in case that a data processor has notified the data breach to you)
Comments on the dates		Optional field; you can provide, if you think nessecary, more information regarding the dates of notification and indicate if you do not know the dates exactly

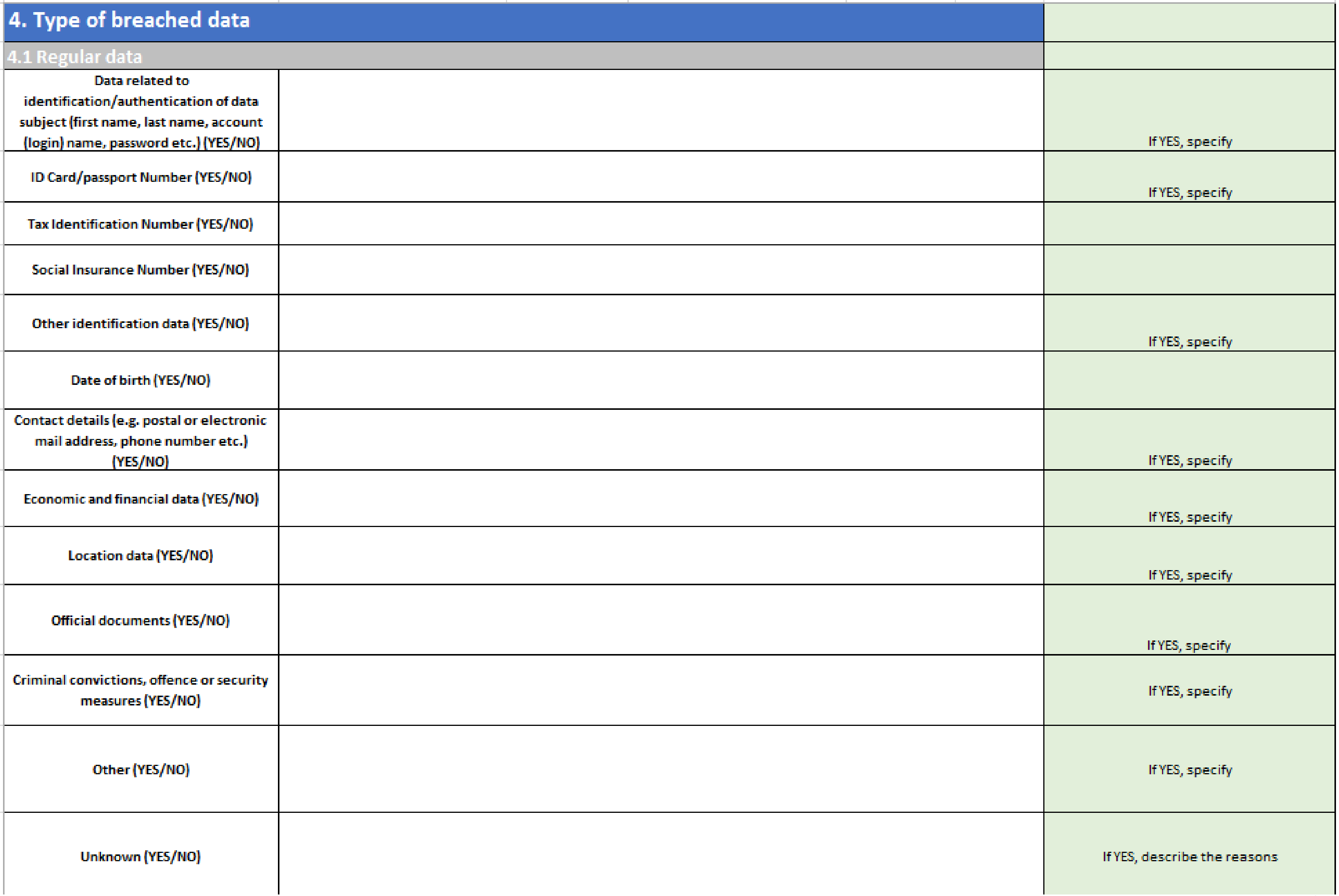
In case that the 72-hours deadline is not being met

The data breach notification form (cont.)



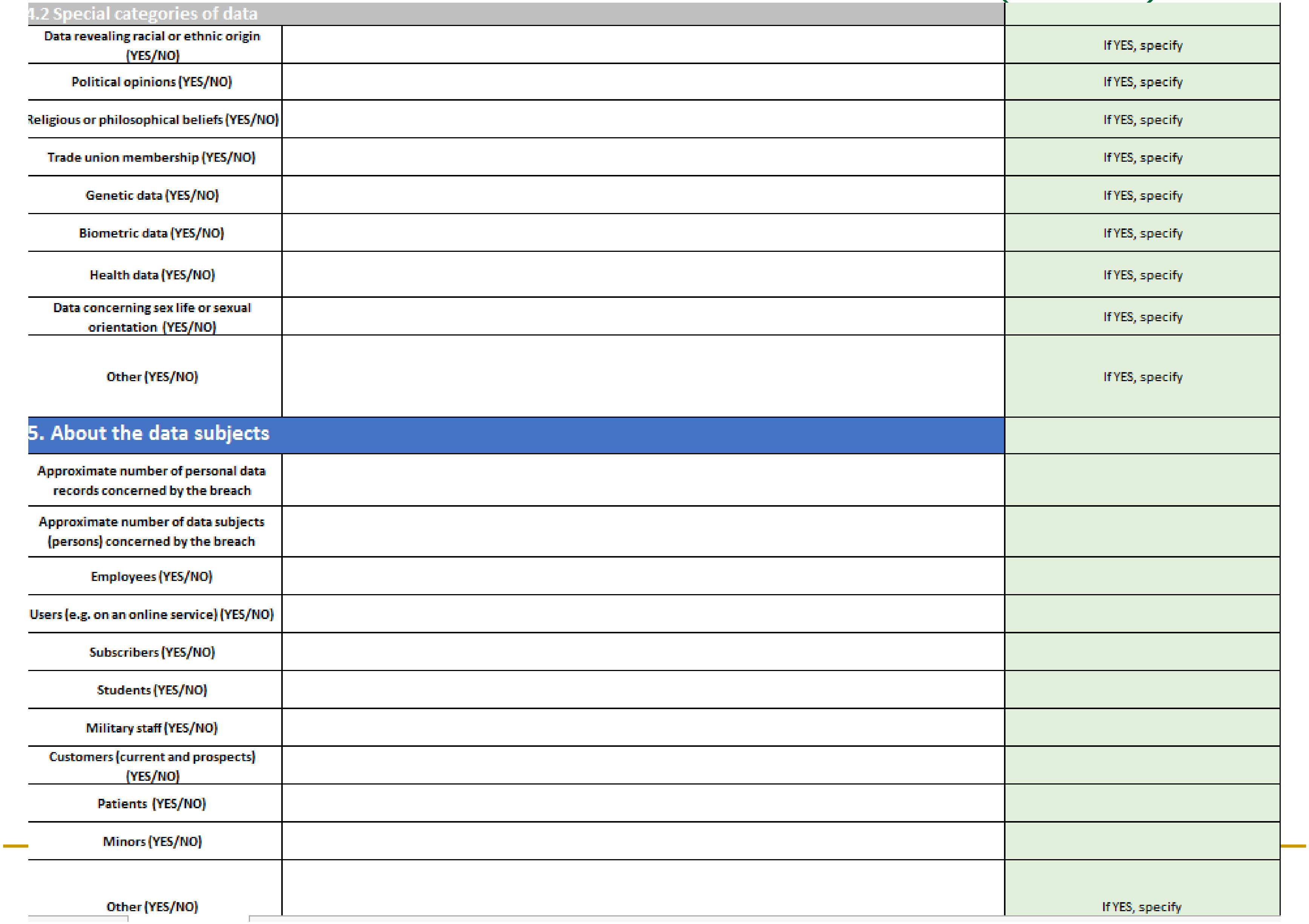
3. About the breach		
Breach of confidentiality? **(YES/NO)**		You fill YES in case of unauthorized disclosure of the data or unauthorized access to the data etc.
Breach of integrity? **(YES/NO)**		You fill YES in case of alteration/modification of data etc.
Breach of availability? **(YES/NO)**		You fill YES in case of loss or destruction of data etc.
Nature of the incident		**Indicative** examples: 1) Device lost or stolen 2) Paper lost or stolen or left in insecure location 3) Mail lost or opened 4) Hacking 5) Malware (e.g. virus, ramsonware) 6) Phishing 7) Incorrect disposal of personal data (either on paper or in electronic format) 8) Unintended publication 9) Data of wrong data subject shown 10) Personal data shown to data recepient 11) Verbal unauthorized disclosure of personal data and others (please specify)
Cause of the breach		**Indicative** examples: 1) Internal non-malicious user 2) Internal malicious user 3) External malicious user 4) Forces of nature (fire, flood, etc.) 5) Obsolete hardware 6) Obsolete software 7) Unknown and others (it may be a combination of the above)

The data breach notification form (cont.)



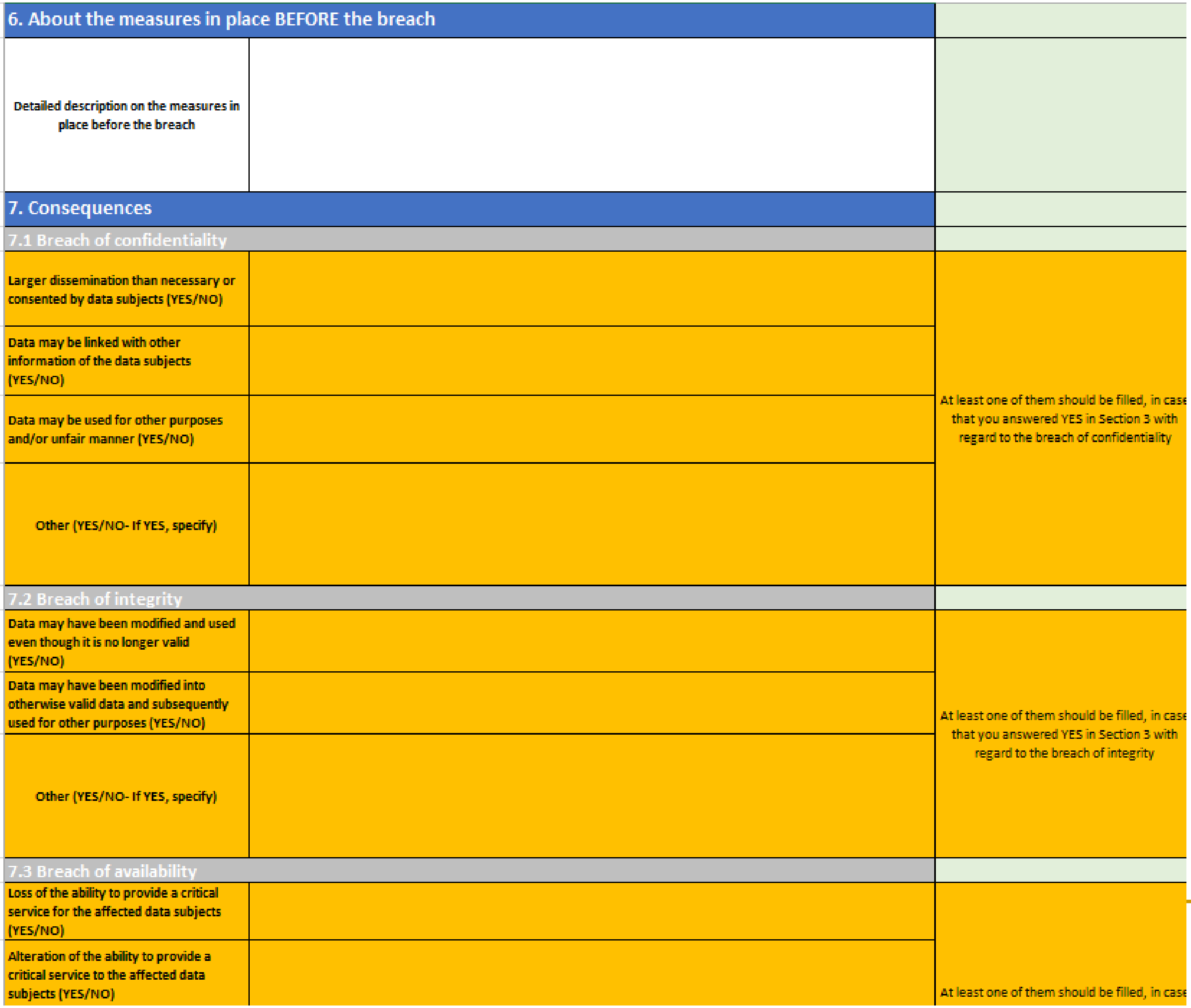
4. Type of breached data		
4.1 Regular data		
Data related to identification/authentication of data subject (first name, last name, account (login) name, password etc.) (YES/NO)		If YES, specify
ID Card/passport Number (YES/NO)		If YES, specify
Tax Identification Number (YES/NO)		
Social Insurance Number (YES/NO)		
Other identification data (YES/NO)		If YES, specify
Date of birth (YES/NO)		
Contact details (e.g. postal or electronic mail address, phone number etc.) (YES/NO)		If YES, specify
Economic and financial data (YES/NO)		If YES, specify
Location data (YES/NO)		If YES, specify
Official documents (YES/NO)		If YES, specify
Criminal convictions, offence or security measures (YES/NO)		If YES, specify
Other (YES/NO)		If YES, specify
Unknown (YES/NO)		If YES, describe the reasons

The data breach notification form (cont.)



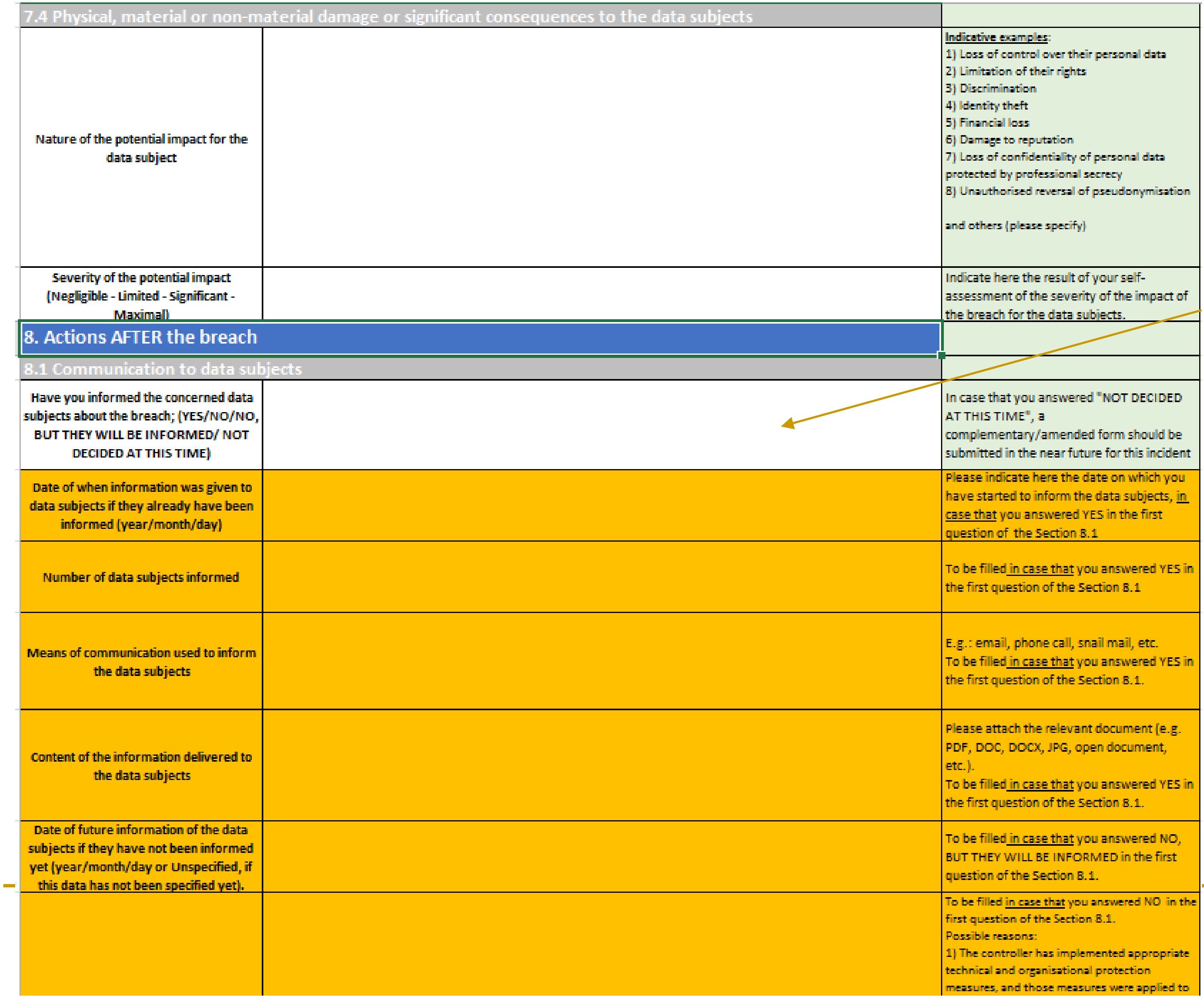
4.2 Special categories of data		
Data revealing racial or ethnic origin (YES/NO)		If YES, specify
Political opinions (YES/NO)		If YES, specify
Religious or philosophical beliefs (YES/NO)		If YES, specify
Trade union membership (YES/NO)		If YES, specify
Genetic data (YES/NO)		If YES, specify
Biometric data (YES/NO)		If YES, specify
Health data (YES/NO)		If YES, specify
Data concerning sex life or sexual orientation (YES/NO)		If YES, specify
Other (YES/NO)		If YES, specify
5. About the data subjects		
Approximate number of personal data records concerned by the breach		
Approximate number of data subjects (persons) concerned by the breach		
Employees (YES/NO)		
Users (e.g. on an online service) (YES/NO)		
Subscribers (YES/NO)		
Students (YES/NO)		
Military staff (YES/NO)		
Customers (current and prospects) (YES/NO)		
Patients (YES/NO)		
Minors (YES/NO)		
Other (YES/NO)		If YES, specify

The data breach notification form (cont.)



6. About the measures in place BEFORE the breach		
Detailed description on the measures in place before the breach		
7. Consequences		
7.1 Breach of confidentiality		
Larger dissemination than necessary or consented by data subjects (YES/NO)		At least one of them should be filled, in case that you answered YES in Section 3 with regard to the breach of confidentiality
Data may be linked with other information of the data subjects (YES/NO)		
Data may be used for other purposes and/or unfair manner (YES/NO)		
Other (YES/NO- If YES, specify)		
7.2 Breach of integrity		
Data may have been modified and used even though it is no longer valid (YES/NO)		At least one of them should be filled, in case that you answered YES in Section 3 with regard to the breach of integrity
Data may have been modified into otherwise valid data and subsequently used for other purposes (YES/NO)		
Other (YES/NO- If YES, specify)		
7.3 Breach of availability		
Loss of the ability to provide a critical service for the affected data subjects (YES/NO)		At least one of them should be filled, in case
Alteration of the ability to provide a critical service to the affected data subjects (YES/NO)		

The data breach notification form (cont.)

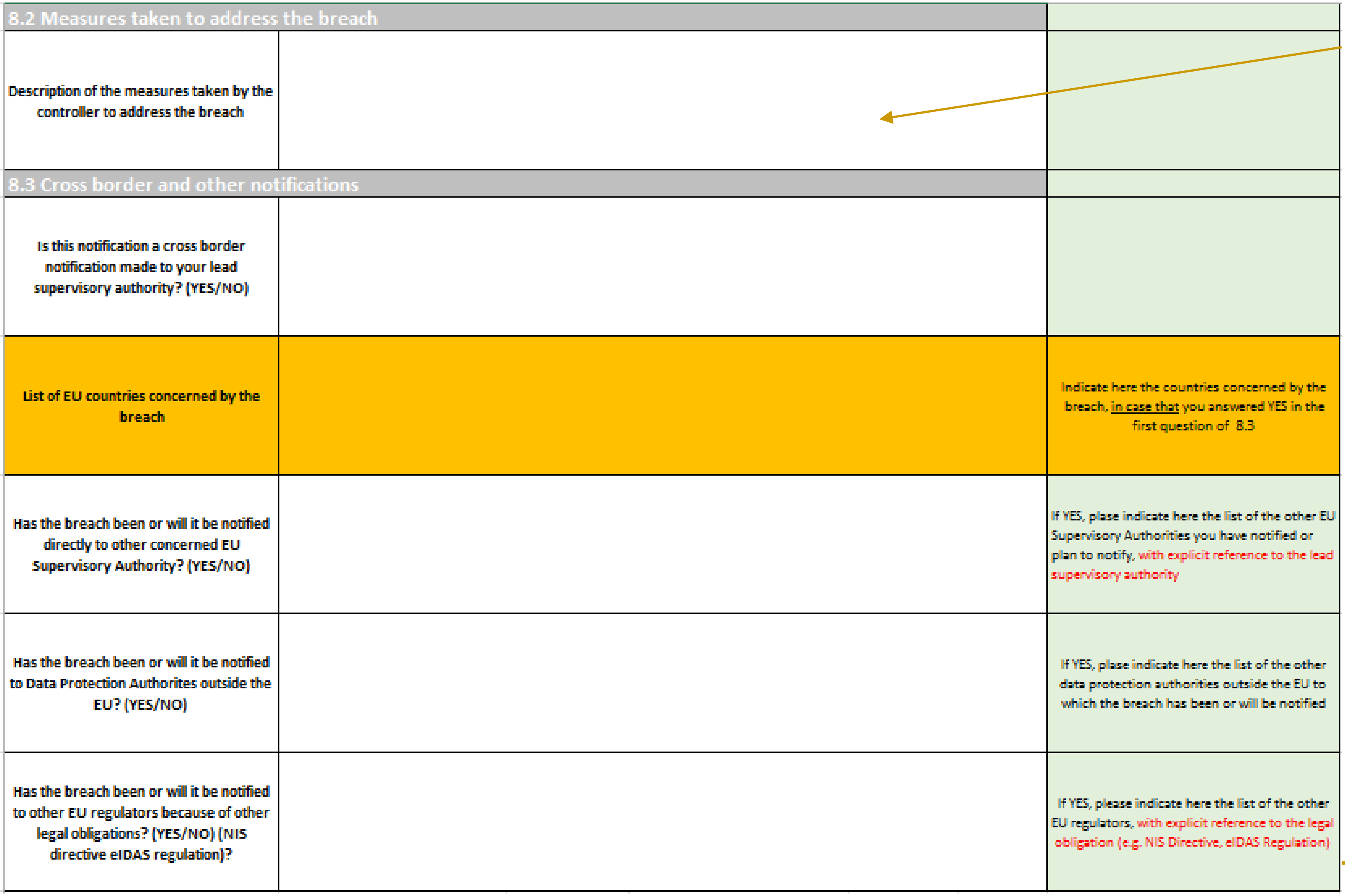


7.4 Physical, material or non-material damage or significant consequences to the data subjects		
Nature of the potential impact for the data subject		Indicative examples: 1) Loss of control over their personal data 2) Limitation of their rights 3) Discrimination 4) Identity theft 5) Financial loss 6) Damage to reputation 7) Loss of confidentiality of personal data protected by professional secrecy 8) Unauthorised reversal of pseudonymisation and others (please specify)
Severity of the potential impact (Negligible - Limited - Significant - Maximal)		Indicate here the result of your self-assessment of the severity of the impact of the breach for the data subjects.
8. Actions AFTER the breach		
8.1 Communication to data subjects		
Have you informed the concerned data subjects about the breach; (YES/NO/NO, BUT THEY WILL BE INFORMED/ NOT DECIDED AT THIS TIME)		In case that you answered "NOT DECIDED AT THIS TIME", a complementary/amended form should be submitted in the near future for this incident
Date of when information was given to data subjects if they already have been informed (year/month/day)		Please indicate here the date on which you have started to inform the data subjects, in case that you answered YES in the first question of the Section 8.1
Number of data subjects informed		To be filled in case that you answered YES in the first question of the Section 8.1
Means of communication used to inform the data subjects		E.g.: email, phone call, snail mail, etc. To be filled in case that you answered YES in the first question of the Section 8.1.
Content of the information delivered to the data subjects		Please attach the relevant document (e.g. PDF, DOC, DOCX, JPG, open document, etc.). To be filled in case that you answered YES in the first question of the Section 8.1.
Date of future information of the data subjects if they have not been informed yet (year/month/day or Unspecified, if this data has not been specified yet).		To be filled in case that you answered NO, BUT THEY WILL BE INFORMED in the first question of the Section 8.1.
		To be filled in case that you answered NO in the first question of the Section 8.1. Possible reasons: 1) The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to

In relation with the assessment on the severity.

The assessment needs to be justified

The data breach notification form (cont.)



8.2 Measures taken to address the breach		
Description of the measures taken by the controller to address the breach		
8.3 Cross border and other notifications		
Is this notification a cross border notification made to your lead supervisory authority? (YES/NO)		
List of EU countries concerned by the breach		Indicate here the countries concerned by the breach, in case that you answered YES in the first question of 8.3
Has the breach been or will it be notified directly to other concerned EU Supervisory Authority? (YES/NO)		If YES, plase indicate here the list of the other EU Supervisory Authorities you have notified or plan to notify, with explicit reference to the lead supervisory authority
Has the breach been or will it be notified to Data Protection Authorities outside the EU? (YES/NO)		If YES, plase indicate here the list of the other data protection authorities outside the EU to which the breach has been or will be notified
Has the breach been or will it be notified to other EU regulators because of other legal obligations? (YES/NO) (NIS directive eIDAS regulation)?		If YES, please indicate here the list of the other EU regulators, with explicit reference to the legal obligation (e.g. NIS Directive, eIDAS Regulation)

Important to proceed immediately with the proper steps

The status so far in Greece

- 33 notifications to the Hellenic DPA since 25/5/2018
  - A small number compared to other Member States
- 11 of them did not result in communicating the breach to the data subjects (no high risk)
- The HDPA provided guidance in almost all cases
  - Especially with regard to communicating the breach to the individuals
- In one case, a complaint filed before the Hellenic DPA by an affected individual regarding a data breach
  - The data controller had already notified the breach to the DPA just a few days before this complaint

Conclusions - Discussion

- Adopt appropriate procedures to allow you efficiently handling personal data breaches
  - The data processor should assist the controller in ensuring compliance with the obligations regarding personal data breaches

- It is crucial to act promptly and take appropriate measures to remedy the consequences as well as to ensure that similar incident is unlikely to occur in the future

- See also:
  - http://www.dpa.gr (Guidelines for controllers -> Personal data breach notification)
  - Guidelines on Personal data breach notification under Regulation 2016/679 (Article 29 Working Party)
  - Recommendations for a methodology of the assessment of severity of personal data breaches (ENISA, 2013)